ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/331412250

Mobile Technology Generations and Cryptographic Algorithms: Analysis Study

Conference Paper · February 2019

CITATIONS
3

READS
613

2 authors:

Khalid Fadhil Jasim
Cihan University-Erbil
12 PUBLICATIONS **37** CITATIONS
SEE PROFILE

Imad Alshaikhli
International Islamic University Malaysia
63 PUBLICATIONS **386** CITATIONS
SEE PROFILE

All content following this page was uploaded by Khalid Fadhil Jasim on 28 February 2019.

The user has requested enhancement of the downloaded file.

Mobile Technology Generations and Cryptographic Algorithms: Analysis Study

Khalid Fadhil Jasim
Department of Computer Science, KICT
International Islamic University Malaysia
Kuala Lumpur, Malaysia
khalid.jassim@yahoo.com

Imad Fakhri Al-Shaikhli
Department of Computer Science, KICT
International Islamic University Malaysia
IIUM Cyber Security Malaysia Center for Cyber Space Security
Kuala Lumpur, Malaysia
imadf@iium.edu.my

***Abstract*—Nowadays, Mobile wireless technologies are becoming more significant and growing rapidly for better features and services. Latest Mobile technologies are expected to provide higher processing power, support high quality multimedia applications, offer reliable wireless connections, faster data transmission rates, and consume less power. At the same time, various mobile generations are susceptible to attack via eavesdropping and information leaking operations. Therefore, some cryptographic algorithms have proposed as confidentiality and integrity algorithms in different mobile generations, in order to prevent or mitigate these harmful operations. This paper provides analysis study of Mobile generations (From Mobile 1G to Mobile 4G) and cryptographic algorithms used in these generations. The study based on some factors like features, services, standards, and techniques which have adopted in these generations.**

Keywords- Mobile Technologies; Cryptographic Algorithms; Mobile Generations; A5/1 Algorithm; SNOW Algorithm;

I. INTRODUCTION

In the past years, Mobile technologies have presented revolution and amazing technical advancement in field of information and communication technology. Mobile technology achieved massive success, and growing progress in wireless communications. Various wireless mobile generations have been established. For instance, First generation of wireless mobile phones (Mobile 1G) introduced in the 1980s, it was based on analog communications and offered voice services without security. In addition, Second generation (Mobile 2G) presented in the 1990s, was based on digital wireless technology, adopted GSM standards, with Time Division Multiple Access (TDMA) and Code Division Multiple Access (CDMA) techniques, and offered some services (e.g. SMS messages, e-mail, and digital fax). Moreover, Third generation wireless technology (Mobile 3G) developed in the 2000s, delivered services of Mobile Broadband technology, adopted different standards such as Universal Mobile Telecommunication System (UMTS) standard, Wideband Code Division Multiple Access (WCDMA) and CDMA2000 technologies. Mobile 3G supported services like video conferencing, digitized voice, multimedia applications, and high speed access to Internet services via mobile networks. Then, Fourth generation (Mobile 4G) introduced faster mobile broadband, adopted Long Term Evolution and Worldwide Interoperability for Microwave Access (LTE and WiMAX) technologies. 4G technology offered services such as IP telephony, HD Mobile TV, Cloud Computing Services, and Mobile Web Access.

Furthermore, in various mobile generations there was a demand to protect mobile systems against the undesired threat operations such as eavesdropping, information leakage, and falsification. Some defense applications have proposed to prevent or mitigate harmful actions against mobile systems. In this context, cryptographic algorithms have presented information security solutions to protect and mitigate threats on these systems. Therefore, some cryptographic algorithms (e.g. A5/1, SNOW, ZUC, and AES) have proposed to achieve information confidentiality, integrity, and authenticity in different mobile generations.

The rest of the paper is organized as follows: we will analyze various mobile generations (Mobile 1G, 2G, 3G, and 4G) in sections II, III, IV, and V respectively. Section VI presents cryptographic algorithms related to mobile generations, based on different factors such as features, services, standards, and techniques have adopted in these generations. Section VII provides analysis summary of mobile generations and cryptographic algorithms. Section VIII gives the conclusion of the paper.

II. FIRST GENERATION OF MOBILE TECHNOLOGY

In the 1980s, first generation (1G) of mobile phone technology appeared. This generation depends on analog radio signals and a higher frequency (150 MHz and up) in the voice modulations. A variety of first generation standards have been used such as Advanced Mobile Phone System (AMPS) and European Total Access Communication Systems (ETACS). The AMPS standards adopted in United States, where radio transmission operations in AMPS system achieved via Frequency Modulation technique (FM) and Frequency Division Duplex technique (FDD). Also, the Frequency Division Multiple Access (FDMA) and 30 KHz for channel bandwidth have been used in AMPS system. Moreover, ETACS system deployed in Europe and it is similar to AMPS standards, but with 25 KHz as a channel

bandwidth and with different format for the Mobile Identification Number [1].

The first generation (1G) possesses some undesirable features such as poor voice connections, low capacity, without security during voice calls and it is intercepted through eaves dropping operations. This analog 1G technology remained in practical use until the appearance of second generation (2G) digital technology [2].

III. SECOND GENERATION OF MOBILE TECHNOLOGY

The second generation of mobile phone technology (2G) introduced in Finland in early 1990s and it was based on Global System for Mobile communication (GSM) standards [3]. The 2G technology adopted two significant standards, Time Division Multiple Access technique (TDMA) and Code Division Multiple Access technique (CDMA). The channel bandwidth (30-200 KHz) and transmission data rate up to 64 kbps have been offered in this technology. In addition, 2G technology relies on digital radio signals, digital coding of voice which enhanced the voice quality and mitigated noisy signals, data compression algorithms of digital voice, and digital encryption algorithms which improved the security via 2G network. Some new services offered by 2G technology, compared with 1G technology, such as short message service (SMS), paging, digital fax, and e-mail.

In late 1990s, the 2.5 generation (2.5 G) developed between second generation and third generation of mobile technology. New standards used in 2.5 G, General Packet Radio Service (GPRS) and Enhanced Data Rates for GSM Evolution (EDGE) standards. GPRS standard adopted packet switching technique for data exchange between the users through mobile networks. Also, GPRS included Multimedia Messaging Services and Wireless Application Protocol. The transmission data rate offered by GPRS standard is (56-115 kbps). Moreover, in 2000, EDGE standard has been deployed [2]. EDGE standard can operates in GSM mobile networks and offers significant characteristics such as high data transmission rate (up to 236 kbps) and more flexibility and reliability compared with GPRS standard. EDGE supports circuit switching data and packet switching data compared with GSM standard. Finally, 2.5 G technology was established to enhance the characteristics of GSM mobile systems via low access time and high data transmission rates, which can be reach up to 384 kbps, and to meet the vast progress of Internet based applications [3].

IV. THIRD GENERATION OF MOBILE TECHNOLOGY

The third generation (3G) is a wireless networks based on international technology and standards, and was established to improve the performance and efficiency of wireless mobile networks. The 3G wireless technology adopted some significant enhancements such as packet data networks, high data transmission speed, and raised the voice and data capacity. Most of 3G wireless networks are compatible with 2G wireless networks technologies (e.g. 3G UMTS, GSM, GPRS, IS-95A/B, 3G CDMA2000 1X and CDMA2000 1xEV). In addition, 3G offered access with high speed to Internet services via mobile networks. This generation included various types of technologies like WCDMA, CDMA2000, UMTS and EDGE [4].

A. WCDMA Technology

The International Telecommunication Union (ITU) has been adopted Wideband Code Division Multiple Access (WCDMA) technology as international standard with the name (IMT-2000). WCDMA used to cover wideband digital communications and supported different services such as videoconferencing, multimedia applications, and Internet based applications. Also, WCDMA offered high data transmission rate up to 2Mbps by using the radio spectrum efficiently. Finally, the 3G wireless networks have been used in United States, Europe, and Japan, and adopted WCDMA technology.

B. CDMA2000 Technology

In 1995, Code Division Multiple Access (CDMA 2000) technology has been deployed. 3G wireless networks used CDMA standard and adopted by International Telecommunication Union (ITU) in 1999. At that time, most of mobile operators evolved their systems from 2G to 3G-CDMA technology in order to improve the capacity of voice traffics, and gain high speed of data transmission. Furthermore, CDMA2000 included CDMA2000 1X and CDMA2000 1xEV-DO (Evolution-Data Optimized) technologies. First, CDMA2000 1X increased the capacity of data and voice services, two times approximately, compared with previous CDMA technology and greater than GSM and TDMA technologies. Also, it supported up to 153 kbps data transmission rate. Secondly, CDMA2000 1xEV-DO supported data services with high speed and high capacity. This technology (with enhanced data version) offered packet data connections, peak data rate up to 2Mbps, and greater than 700 kbps as throughput. Thus, it is supported huge size file download applications, and videoconferencing via mobile wireless networks.

C. UMTS Technology

In 2002, Universal Mobile Telecommunication System (UMTS) has been launched as standard for 3G wireless networks and adopted by the European Telecommunications Standards Institute (ETSI). UMTS offered high speed transmission rate (2Mbps), which is more than previous generations (i.e. 1G, 2G, and 2.5 G). This standard has been supported packet switching technique and circuit switching technique at the same time. When UMTS technology is available, users can access Internet resources while they are roaming and traveling around the world, and can using different combinations of satellite and terrestrial wireless communication systems. UMTS also offered various services through mobile networks (e.g. video conferencing, digitized voice, and multimedia applications) [5].

V. FOURTH GENERATION OF MOBILE TECHNOLOGY

The fourth generation of mobile communication technology (4G) has been appeared after third generation technology (3G). 4G technology supported Mobile Broadband Internet Access, therefore some devices (e.g. Smart phones, laptops with wireless cards,…) can access Internet resources via this technology. Also, this technology offered various services like IP telephony, HD Mobile TV, Cloud Computing Services, and Mobile Web Access. Moreover, the 4G mobile technology included Worldwide Interoperability for Microwave Access (WiMAX) standard and Long Term Evolution (LTE) standard. In 2010, Mobile WiMAX and LTE standards have been adopted as 4G technology and recognized by International Telecommunication Union (ITU) [6].

A. WiMAX Technology

In 2007, the WiMAX standard has been adopted in South Korea, then in 2008 used in United States by Sprint Corporation (Formerly, Clearewire). The WiMAX technology has been used for fixed broadband wireless access and adopted IEEE 802.16 standard. The speed, in case of fixed stations, is up to 40 Mbps (1 Gbps, in future). WiMAX also offers broadband wireless access up to 30 miles in fixed stations and 3-10 miles in case of mobile stations [7]. Furthermore, the bandwidth is (1.25-20 MHz), frequency-division duplex (FDD) and time-division duplex (TDD) operations are supported in WiMAX. Orthogonal Frequency Division Multiplexing (OFDMA) is used in uplink and downlink data transmission operations. Multiple antenna technologies have been used in Mobile WiMAX, multi user MIMO(Multiple-Input Multiple-Output) and single user MIMO are supported for transmissions operations as well [8].

B. LTE Technology

The Long Term Evolution (LTE) has been developed based on previous 3G technology (UMTS/ HSDPA). In 2009, the LTE technology adopted in Scandinavian cities Oslo and Stockholm. In 2012, LTE services have been deployed in United States by various mobile operators. In addition, frequency bandwidth offered in LTE technology was (1.4-20 MHz). Orthogonal Frequency Division Multiplexing (OFDMA) modulation technique used for downlink transmission and for uplink transmission Single Carrier Frequency Division Multiple Access (SDMA) has been used. FDD and TDD were supported in this technology as well. Furthermore, LTE offered peak data rates (100-326.4 Mbps) in downlink and (50 Mbps) for uplink data transmissions operations, based on the antenna technology and modulation technique. Multiple antenna technologies have been adopted in LTE such as MIMO, Beam forming, and Spatial Division Multiple Access. As a result, using multiple antenna techniques in LTE technology increased data transmission rates, capacity, and efficiency of mobile systems [9].

VI. CRYPTOGRAPHIC ALGORITHMS

Cryptographic algorithms are cryptography techniques used to address some information security issues in various Mobile Generations (2G, 3G, and 4G). In this section, we will analyze and investigate some cryptography algorithms such as A5/1, SNOW, ZUC, and AES.

A. A5/1 Algorithm

The security of voice calls and data transmissions via mobile communications represents crucial issue for most of mobile users. A5/1 cryptography algorithm proposed to support data authentication and data encryption in second generation GSM mobile systems (2G-GSM) [10]. This algorithm has been adopted as encryption algorithm to secure data transmission operations in GSM systems. Moreover, A5/1 algorithm classified as stream cipher, it relies on three Linear Feedback Shift Registers (R1, R2, and R3) and 64-bits key (Kc). Lengths of registers R1, R2, and R3 are 19 bits, 22 bits, and 23 bits respectively. The three registers (R1, R2, and R3), of A5/1 algorithm, are clocked 224 times then produce two (114-bits) as output key streams. The first generated 114-bits of key stream denoted by BLOCK1, and the second 114-bits denoted by BLOCK2. BLOCK1 (114-bits) is employed to encipher the uplink transmission and BLOCK2 (114-bits) to decipher the downlink transmission at Mobile Station Side. Also, BLOCK1 (114-bits) is employed to decipher the uplink transmission and BLOCK2 (114-bits) to encipher the downlink transmission at Network Side. Thus, plaintexts in this cryptography system are arranged as groups of (114-bits) and according to Time Division Multiple Access technology [11].

B. SNOW3G Algorithm

SNOW 3G algorithm represents the confidentiality algorithm in (3G-UMTS) mobile generation systems [12]. It is a stream cipher, which consists of Linear Feedback Shift Register (LFSR[S0,S1, … ,S15]), and finite state machine (FSM) which also includes three registers R1[32-bit], R2[32-bit] and R3[32-bit]. In addition, substitution boxes S1(32x32-bit) and S2(32x32-bit) are used in this stream cipher. SNOW 3G relies on secret key (128-bit) and initialization variable IV (128-bit) during initialization operation of main components of this algorithm. After initialization operation is achieved, the algorithm is moved without generating output bits. Then in generating operation, with each clock it generates 32-bit word as keystream. Usually, this keystream is used in encryption and decryption operations of plaintexts and ciphertexts respectively [13].

C. ZUC Algorithm

The confidentiality algorithm (128-EEA3) and integrity algorithm (128-EIA3) have been adopted for the security of fourth generation (4G-LTE) technology. Confidentiality Key (CK with 128-bit) and Integrity Key (IK with 128-bit) used in these algorithms. The two algorithms are based on ZUC stream cipher algorithm [14]. Moreover, ZUC algorithm used initial Key K (128-bit) and Initial Vector IV (128-bit)

[15]. The structure of ZUC algorithm is relied on Linear Feedback Shift Register (LFSR [S0,S1, … ,S15], where each word of S0, … , S15, contains 31-bit). Bit Reorganization (BR) operation is used after LFSR, where 8 (16-bit) values are taken from the positions (S0, S2, S5, S7, S9, S11, S14, and S15) of LFSR, rearranged these values to produce 4 (32-bit) words denoted by X0, X1, X2, and X3. Furthermore, the nonlinear Function F comprises Substitution box S (S-box S), and two memory cells Registers (R1 [32-bit], and R2 [32-bit]). S-box S includes S-box S0 (with 8-bit input, and 8-bit output), and S-box S1 (with 8-bit input, and 8-bit output). The values of words X0, X1, and X2 are selected as input to the function F, and F will produce word W (32-bit) as output. The key stream (Z, 32-bit word) is generated by exclusive or W with X3 (Z=W XOR X3). Finally, the confidentiality algorithm (128-EEA3) adopted to encrypt user data in Packet Data Convergence Protocol (PDCP which is part of Layer 2 in LTE protocol), where it is used to encipher transmitted data (at IP packets, uplink transmission) and decipher received data (at PDCP protocol, downlink) [16, 17].

D. AES Algorithm

For the security of Long Term Evolution (LTE), the confidentiality algorithm (128-bit EEA2) and integrity algorithm (128-bit EIA2) have been adopted as the second set in (4G-LTE) mobile networks. EEA2/EIA2 algorithms are based on Advanced Encryption Standard Algorithm (128-bit AES with 10 Rounds). AES is a block cipher algorithm which relies on 128-bit data block, user secret keys of lengths 128-bit, 192-bit, and 256-bit [18]. Moreover, AES algorithm (128-bit AES) includes two main significant tasks, the state updating transformation and Key scheduling. In state update task, the input data to AES partitioned into blocks and each block contains 128-bit. Then input data block (128-bit) is arranged as 16 bytes and organized in two dimension array of size (4x4). The following operations are performed to update the state of AES-128 algorithm:

- **SubBytes Operation:** It is a non linear transformation where each of 16 bytes is used as input to S-box (8-bit) and produce new byte (final output of new16 bytes).
- **ShiftRows Operation:** It is a cyclic permutation where each row (i) in array (4x4) is rotated to left by i positions (i=0,1, 2, 3) [19].
- **MixColumns Operation:** It is a linear diffusion where each column of array (4x4) is multiplied by constant MDS matrix.
- **AddRoundKey Operation:** AES-128 consists of 10 Rounds, thus in Round(i) the Round Key RK_i (128-bit) is added to the 16 bytes contained in array (4x4) [20].

Furthermore, in key schedule task of AES-128, round key RK0 is taken from master key (128-bit) used in AES-128 algorithm. Then each round key RKi (with i=1,2, … ,10) is produced based on its predecessor RKi-1 [21].

VII. DISCUSSION

The analysis summary of mobile generations and cryptographic algorithms, shown in (TABLE 1 and TABLE 2), are as follows:

- First Generation has been established the idea of seamless mobile networks and presented voice services via mobile networks. But, there are limitations such as Mobile 1G relies on analog transmission technique which is not efficient and it depends on limited spectrum, needs large frequency gap between users to prevent communication interference. Also, analog mobile devices consume more power, heavy devices and need high cost. Mobile 1G (AMPS, NMT, TACS standards) offers one user per radio communication channel (30 KHz).
- Second Generation introduced digital wireless mobile technology and expanded voice capacity (i.e. offered voice services for more users in more places). Mobile 2G offered digital transmission, compressed voice, and multiuser per channel. Also, digital devices possess low cost and weight, and provide more security. At the same time, limitations raised in mobile 2G such as it also needs large frequency gap between mobile users to decrease the communication interference. Mobile 2G (with D-AMPS standard and based on TDMA technique) offers 3 users per radio communication channel (30 KHz), and Mobile 2G (with GSM standard and based on TDMA technique) offers 8 users per radio communication channel (200 KHZ).
- Third Generation delivered services of Mobile Broadband technology. Mobile 3G also offered high speed Internet services and better mobile connections. Moreover, in Mobile 3G with CDMA technique (Code Division Multiple Access), voice capacity has been expanded several times, spectrum resources utilized efficiently, battery life raised in mobile devices, and offered better secure communication (based on CDMA encoding). Furthermore, 3G technology delivered high data rates, for instance 3G (with CDMA2000, EV-DO standards) offered peak data rate (3.1 to 14.7 Mbps) , and 3G (with WCDMA, HSPA standards) offered peak data rate (14.4 to 63+ Mbps). But, in 2G (GSM, GPRS standards) peak data rate was (less than 0.5 Mbps).
- Fourth Generation presented additional capacity, faster mobile broadband, and better mobile experiences. Mobile 4G increased data capacity, supported wider channel bandwidths (up to 20 MHz with OFDMA technique). 4G offered data rates (300+ Mbps). Also, 4G adopted multiple antenna technologies, and advanced MIMO techniques to improve data transmission rates,

capacity, and efficiency of mobile systems. Moreover, Mobile 4G, during real time connection, relies on simple core network, flattened architecture (in all IP network), needs less equipment, and low latencies with optimized time-response for plane control and user.

- Cryptographic Algorithms: Symmetric cryptography algorithms [22] adopted to protect sensitive information transmitted through different Mobile technologies. Mobile 1G was without security during voice calls and it was intercepted through eavesdropping operations. Moreover, for Mobile 2G (with GSM standard), A5/1 cryptography algorithm used to support data authentication and data encryption. Stream cipher, SNOW 3G algorithm, adopted as confidentiality and integrity algorithms in Mobile 3G (3G with UMTS standards). The confidentiality and integrity algorithms (128-EEA3 and 128-EIA3) proposed for the security of Mobile 4G (4G with LTE standard) technology, these two algorithms were based on ZUC cryptography algorithm. Furthermore, the confidentiality algorithm (128-bit EEA2) and integrity algorithm (128-bit EIA2) have been used for the security of Mobile 4G (with LTE standard). Algorithms (128-EEA2and 128-EIA2) were based on Advanced Encryption Standard Algorithm (128-bit AES with 10 Rounds).

TABLE 1: MOBILE GENERATIONS AND CRYPTOGRAPHIC ALGORITHMS

Mobile Technology	Features	Services	Speed (Data Rates)	Standards	Encryption Algorithms
Mobile(1G)	-Appeared in 1980s -Used analog radio signals -Analog wireless cellular technology	Provided analog voice signals Without data services	Up to 2.4 kbps	AMPS ETACS	Without encryption
Mobile(2G)	-Introduced in 1990s -Used digital radio signals -Digital wireless network -Digital coding of voice -Data compression algorithms of digital voice -Raised voice and data capacity	-Provide digital voice and SMS message -Enhanced voice quality -Supported MMS and Internet Connections -Paging, digital fax, and e-mail.	Up to 64 kbps	GSM TDMA CDMA	A5/1 algorithm
Mobile(3G)	-Introduced in 2000 -Digital broadband network -Fast data transfer rate -Improved spectral efficiency -Greater network capacity	-Enhanced audio and video streaming - Video conferencing - Support web browsing at higher speed and IP TV	Up to 2Mbps	WCDMA CDMA2000 UMTS EDGE	SNOW 3G algorithm
Mobile(4G)	-Introduced around the year 2010 -Digital broadband packet -Converged data and voice over IP -Entirely packet switched network -Higher bandwidth to provide multimedia applications	-Enhanced audio and video streaming -IP telephony and HD mobile TV -Gaming services, 3D TV, and Cloud computing	200 Mbps to 1 Gbps	LTE LTE(advanced) WiMAX	ZUC algorithm AES algorithm

TABLE 2: ANALYSIS SUMMARY

Mobile Technology	Analysis Summary
Mobile(1G)	-Established the idea of seamless mobile networks -Relies on analog transmission technique - Depends on limited spectrum - Needs large frequency gap between users to prevent communication interference - Analog mobile devices consume more power - Heavy devices and need high cost - Without security during voice calls and it was intercepted through eavesdropping operations
Mobile(2G)	- introduced digital wireless mobile technology - Expanded voice capacity - Offered digital transmission and compressed voice - Digital devices possess low cost and weight - needs large frequency gap between mobile users to decrease the communication interference - A5/1 cryptography algorithm used to support data authentication and data encryption -
Mobile(3G)	- Delivered services of Mobile Broadband technology - Offered high speed Internet services - Better mobile connections -Expanded voice capacity several times - Spectrum resources utilized efficiently - Offered better secure communication (based on CDMA encoding) - Offered peak data rate (14.4 to 63+ Mbps) - Adopted SNOW 3G as confidentiality and integrity algorithms
Mobile(4G)	- Presented faster mobile broadband -Better mobile experiences - Increased data capacity -Supported wider channel bandwidths (up to 20 MHz with OFDMA technique) - Offered data rates (300+ Mbps) - Adopted multiple antenna technologies -Relies on simple core network, flattened architecture (in all IP network) - Adopted ZUC and AES as confidentiality and integrity algorithms

VIII. CONCLUSION

This paper provided analysis study of cryptographic algorithms and Mobile technologies from First Generation (1G) to Fourth Generation (4G) based on features, services, standards, techniques, and confidentiality and integrity algorithms offered by each mobile generation. Mobile 1G presented seamless mobile networks, relied on analog technology, and was without security during voice calls. Mobile 2G adopted digital wireless technology, compressed voice, expanded voice capacity, peak data rate (less than 0.5 Mbps), and A5/1 cryptography algorithm used to support data authentication and data encryption (in 2G with GSM standard). Mobile 3G introduced Mobile Broadband technology, supported high speed Internet services, voice capacity expanded several times, delivered high data rates (63+ Mbps), and delivered better secure communication (based on CDMA encoding). SNOW 3G algorithm used as confidentiality and integrity algorithms in Mobile 3G (3G with UMTS standards). Mobile 4G offered faster mobile broadband, wider channel bandwidths (up to 20 MHz with OFDMA technique), data rates (300+ Mbps), adopted multiple antenna technologies, and advanced MIMO techniques. ZUC and AES cryptography algorithms have been used for the security of Mobile 4G (with LTE standard).

REFERENCES

[1] C. S. Patil, R. R. Karhe, and M. A. Aher, "Development of Mobile Technology: A Survey," International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, vol. 1, no. 5, pp. 374–379, 2012.

[2] S. Shukla, V. Khare, S Garg, and P. Sharma, "Comparative Study of 1G , 2G , 3G and 4G," Journal of Engineering, Computers & Applied Sciences (JEC&AS), vol. 2, no. 4, pp. 55–63, 2013.

[3] M. R. Bhalla and A. V. Bhalla, "Generations of Mobile Wireless Technology: A Survey," International Journal of Computer Applications, vol. 5, no. 4, pp. 26–32, 2010.

[4] M. J. Arshad, A. Farooq, and A. Shah, "Evolution and Development Towards 4 th Generation (4G) Mobile Communication Systems," Journal of American Science, vol. 6, no. 12, pp. 63–68, 2010.

[5] M. La Polla, F. Martinelli, and D. Sgandurra, "A Survey on Security for Mobile Devices," IEEE Communications Surveys & Totorials, no. November 2011, pp. 1–26, 2012

[6] R. Sood and A. Garg, "Digital Society from 1G to 5G: A Comparative Study," International Journal of Application or Innovation in Engineering & Management (IJAIEM), vol. 3, no. 2, pp. 186–193, 2014.

[7] S. More and D. K. Mishra, "4G Revolution: WiMAX technology," Third Asian Himalayas Int. Conf. Internet, pp. 1–4, November 2012.

[8] F. Rezaei, M. Hempel, and H. Sharif, "A comprehensive performance analysis of LTE and Mobile WiMAX," 8th Int. Wirel. Commun. Mob. Comput. Conf., pp. 939–944, Aug. 2012.

[9] V. H. Muntean and M. Otesteanu, "WiMAX versus LTE - An overview of technical aspects for next generation networks technologies," 9th Int. Symp. Electron. Telecommun., pp. 225–228, November 2010.

[10] A. Mahalanobis and J. Shah, “An Improved Guess-and-Determine Attack on the A5 / 1 Stream Cipher,” Journal of Computer and Information Science, vol. 7, no. 1, pp. 115–124, 2014.

[11] M. Kalenderi, D. Pnevmatikatos, I. Papaefstathiou, and C. Manifavas, “Breaking the GSM A5/1 cryptography algorithm with rainbow tables and high-end FPGAs,” in Proceedings - 22nd International Conference on Field Programmable Logic and Applications, FPL 2012, pp. 747–753.

[12] B. Debraize and I. M. Corbella, “Fault analysis of the stream cipher snow 3G,” in Fault Diagnosis and Tolerance in Cryptography - Proceedings of the 6th International Workshop, FDTC 2009, pp. 103–110.

[13] J. Molina-Gil, P. Caballero-Gil, C. Caballero-Gil, and A. Fúster-Sabater, "Analysis and Implementation of the SNOW 3G Generator Used in 4G/LTE Systems," in *International Joint Conference SOCO’13-CISIS’13-ICEUTE’13*. vol. 239, Á. Herrero, B. Baruque, F. Klett, A. Abraham, V. Snášel, A. C. P. L. F. Carvalho, *et al.*, Eds., ed: Springer International Publishing, pp. 499-508, 2014.

[14] O. Markowitch and D. Van Heule, “SAT Based Analysis of LTE Stream Cipher ZUC,” ACM, SIN ’13, November 26-28, 2013, Aksaray, Turkey, pp. 110–116.

[15] Zhang, Lingchen, et al., “Evaluating the Optimized Implementations of SNOW3G and ZUC on FPGA”, Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on. IEEE, 2012.

[16] S. Traboulsi, N. Pohl, J. Hausner, A. Bilgic, and V. Frascolla, “Power analysis and optimization of the ZUC stream cipher for LTE-Advanced mobile terminals,” in 2012 IEEE 3rd Latin American Symposium on Circuits and Systems, LASCAS 2012 - Conference Proceedings.

[17] Wu, Hongjun, et al. "Differential attacks against stream cipher zuc." Advances in Cryptology–ASIACRYPT 2012. Springer Berlin Heidelberg, pp. 262-277, 2012.

[18] G. Orhanou, S. El Hajji, and Y. Bentaleb, “EPS AES-based confidentiality and integrity algorithms: Complexity study,” in International Conference on Multimedia Computing and Systems - Proceedings, 2011.

[19] R. Jain, R. Jejurkar, S. Chopade, S. Vaidya, and M. Sanap, "AES Algorithm Using 512 Bit Key Implementation for Secure Communication," *International Journal of Innovative Research in Computer and Communication Engineering,* vol. 2, pp. 3516-3522, 2014.

[20] Tunstall, Michael, “Practical complexity differential cryptanalysis and fault analysis of AES”, Journal of Cryptographic Engineering 1.3, pp. 219-230, 2011.

[21] D. Gstir and M. Schl, “Fast Software Encryption Attacks on AES,” AFRICACRYPT 2013, LNCS 7918, pp. 359–374, 2013.

[22] T. Gunasundari and K. Elangovan, "A Comparative Survey on Symmetric Key Encryption Algorithms," *International Journal of Computer Science and Mobile Applications*, vol. 2, pp. 78-83, 2014.

View publication stats